AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of

7541 South Mingo Road, Apartment #3119, Tulsa, Oklahoma; a 2006 Toyota Scion two-door coupe bearing Oklahoma tag CZM-657 VIN # JTKDE167060070600 ; and a white 2013 Landrover 4-door Oklahoma license plate GTD626 VIN # SALVR2BG7DH855411

Case No. 19-MJ-167-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A":

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	
18 U.S.C. § 1028(a)(2)	**Unlawful Transfer of a Document or an Authentication Feature**
18 U.S.C. § 1028(a)(3)	**Unlawful Transfer of a Document or an Authentication Feature**
	Possession With Intent to Use or Transfer Five or More Documents or Authentication Features
18 U.S.C. § 1028(a)(7)	**Unlawful Transfer, Possession, or Use of a Means of Identification**
18 U.S.C. § 1028A	**Aggravated Identity Theft**
18 U.S.C. § 1343	**Wire Fraud**
8 U.S.C. § 1326	**Reentry of Removed Alien**

The application is based on these facts:

See Affidavit of Homeland Security Investigations Special Agent Dustin Carder attached hereto.

- ☑ Continued on the attached sheet.
- ☐ under 18 U.S.C. ___ days (give exact ending date if more than 30 _____) is requested

under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

DUSTIN CARDER, SPECIAL AGENT

Printed name and title

Sworn to before me and signed in my presence.

Date: 8-22-2019

Judge's signature

City and state: Tulsa, OK Tulsa, Oklahoma

The Honorable Jodi F. Jayne, U.S. Magistrate

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Dustin Carder, being duly sworn, declare and state as follows:

EXPERIENCE AND TRAINING

1. I am a Special Agent employed by Homeland Security Investigations (HSI). I have been employed as a special agent since December 2018. Prior to becoming a special agent, I was employed as a deputy sheriff with the Tulsa County Sheriff's Office in Tulsa, Oklahoma for over twelve (12) years. During my tenure as a deputy sheriff, I spent over six (6) years on patrol where I conducted numerous criminal investigations, made hundreds of arrests, and conducted interviews of suspects, victims, and witnesses. Prior to becoming a HSI Special Agent, I was a Task Force Officer (TFO) with HSI for approximately two and a half years. While on the task force, I conducted and/or assisted in investigations involving narcotics trafficking, bulk cash smuggling, child exploitation, organized criminal activity, and the manufacture and distribution of fraudulent documents. I am a graduate of the Federal Law Enforcement Training Center's (FLETC) twelve-week Criminal Investigator Training Program (CITP) and the sixteen-week Homeland Security Investigations Special Agent Training (HSISAT) program. During the HSISAT program, I received specific training on HSI's programmatic areas of enforcement, including document and benefit fraud. Prior to beginning my career in law enforcement, I received a Bachelor of Arts in Psychology degree in 2005.

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit including:

a. the entire property located at **7541 South Mingo Road, Apartment #3119, Tulsa, Oklahoma** (herein after known as the "**SUBJECT PREMISES**");

b. a 2006 Toyota Scion two-door coupe bearing Oklahoma tag CZM-657, VIN # JTKDE167060070600 (the "**SCION**");

c. a white 2013 Landrover 4-door Oklahoma license plate GTD626, VIN # SALVR2BG7DH855411 (the "**LANDROVER**" together with the SCION the "**VEHICLES**").

and the content of electronic storage devices located therein, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1028(a)(2) (Unlawful Transfer of a document or Authentication Feature); 18 U.S.C. § 1028(a)(3) (Possession With Intent to Use or Transfer Five or More documents or Authentication Features); and 18 U.S.C. § 1028(a)(7) (Unlawful Transfer, Possession, or Use of Means of Identification); 18 U.S.C. § 1028A (Aggravated Identity Theft); 18 U.S.C. § 1343 (Wire Fraud) which items are more specifically described in Attachment B of this Affidavit.

3. The statements in this affidavit are based in part on information provided by HSI agents/task force officers in Tulsa, Oklahoma, confidential informants (CI), forensic document examiners at the HSI Forensic Document Laboratory (FDL), the Tulsa Police Department (TPD) and on your affiant's investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing search warrants, your affiant has not included each and every fact known to him concerning this investigation. Your affiant has set forth only the facts that he believes are necessary to establish probable cause to believe that contraband and evidence, fruits,

and instrumentalities of violations of the aforementioned crimes are presently located at the **SUBJECT PREMISES** and the **VEHICLES**.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 1028(a)(2) prohibits a person from knowingly transferring an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority.

b. Title 18, United States Code, Sections 1028(a)(3) prohibits a person from knowingly possessing with intent to use unlawfully or transfer unlawfully five or more identification documents, authentication features, or false identification documents.

c. Title 18, United States Code, Sections 1028(a)(7) prohibits a person from knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

d. Title 18, United States Code, Sections 1028A prohibits a person during and in relation to any felony violation enumerated in subsection (c), that knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person.

e. Title 18, United States Code, Sections 1343 prohibits a person having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

PROBABLE CAUSE

5. In December 2017, HSI Tulsa began investigating the manufacturing and distribution of fraudulent immigration and state identification documents in the Northern District of Oklahoma. HSI Tulsa agents had learned from a Confidential Informant #1 (CI-01) that a subject identified as **Christian ALVARADO Morales** was acting as a document vendor, selling fraudulent documents. **ALVARADO** provided his phone number as (918) 955-1429 to CI-01 as the number customers would need to call to obtain the fraudulent documents.

6. HSI agents conducted various databases queries and records checks on **ALVARADO** and discovered that he was arrested February 2008 in Tulsa, Oklahoma, on state charges for Make/Sell/Possess/Display False ID, and Violation of Computer Crimes Act by the Tulsa Police Department.

7. Records checks further revealed that **ALVARADO** is a citizen and national of Mexico who had been in the country illegally. **ALVARADO** was convicted of the state charges of Make/Sell/Possess/Display False ID, and Violation of Computer Crimes Act and given a three-year suspended sentence. **ALVARADO** was subsequently removed from the United States

on March 25, 2008 by Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO).

8. In August 2018, HSI Tulsa agents Darren Collins, Dustin Carder, and Tulsa County Sheriff's Office (TCSO) Investigator Ricardo Vaca (acting as translator) placed a consensual recorded phone call to (918) 955-1429 utilizing Confidential Informant #2 (CI-02). CI-02 called the number and spoke with a male voice. CI-02 asked the subject about obtaining identification documents and what the process was for purchasing them. The subject explained that he could provide a driver's license and social security card, $120 for both, and a ten-year Permanent Resident card for $150. The subject stated that CI-02 would need to text him a picture, name and address for the IDs; once they are made, they would then meet to conduct the transaction. CI-02 then told the subject that CI-02 does not get paid until next week and would contact him then.

9. On August 6, 2018, HSI Tulsa, with the assistance of TCSO Deputy Vaca, sent a text message to (918) 955-1429 with fictitious information (i.e. name, date of birth, and address) along with a photograph so that the documents could be made. On August 7, 2018, CI-02 made a consensual recorded phone call to (918) 955-1429 and was instructed by the subject to go to a parking lot near 6100 South Memorial Drive in Tulsa. CI-02 was further instructed to call him back when they got there.

10. HSI agents and TCSO Deputy Vaca briefed CI-02 near the meet location and provided CI-02 with $270 in cash, with which to make the purchase. Surveillance set up in the area prior to CI-02's arrival. CI-02 was followed to the location by HSI SA Dustin Carder and TCSO Deputy Vaca. CI-02 arrived at the location at approximately 1900 hours and called the

subject at (918) 955-1429 and informed him that they were at the location. A few minutes later, the subject arrived in the **SCION** and pulled up to the driver's side of CI-02's vehicle. A hand-to-hand exchange took place without either party exiting their vehicles and lasted only seconds. HSI SA Darren Collins was able to observe the subject and confirmed that it was **Christian ALVARADO Morales**, based on previous surveillance and his photograph from his immigration A-file. (See photo below: **ALVARADO** did not exit the vehicle)

11. HSI SA Collins, Carder and TCSO Deputy Vaca met with CI-02 after the transaction. CI-02 stated that **ALVARADO** only charged $150; he gave CI-02 a social security card and a Permanent Resident Card with the previously provided fictional information from HSI Tulsa but he did not provide a driver's license as requested.

12. HSI SA Carder queried the number on the social security card, 461-36-4475, using investigative database tool Consolidated Lead Evaluation and Recording (CLEAR).

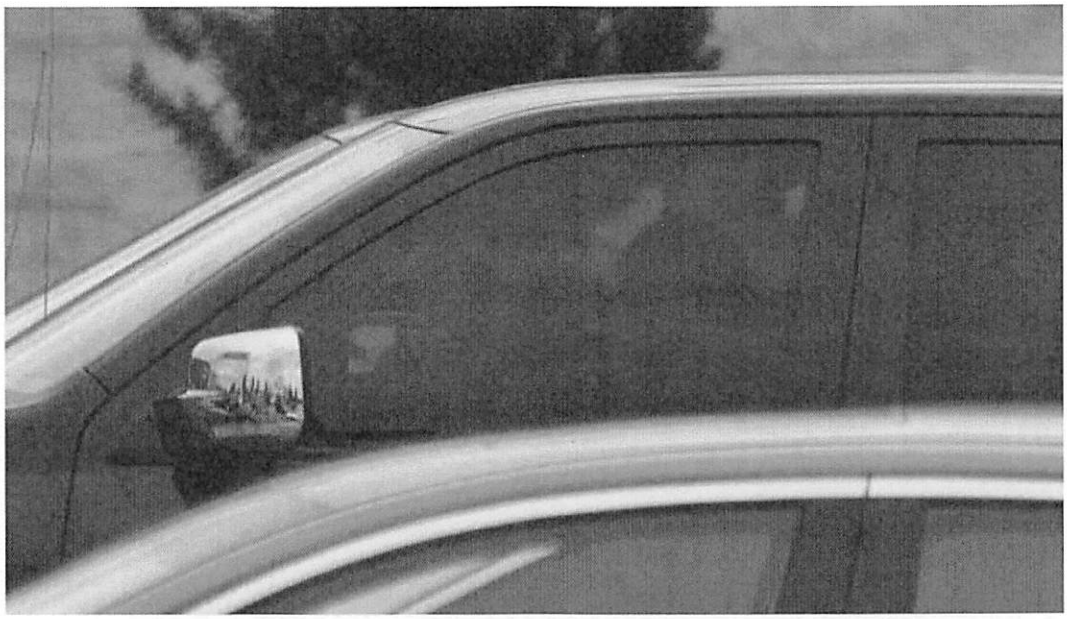
CLEAR shows the number belongs to a Rex Matthews DOB: 1/25/1929, who died on 7/30/2013. The Permanent Resident card had USCIS number 094-981-334. HSI SA Michael Lelecas queried the USCIS database for that number. The number checked to a Juan Banuelas-Chavez DOB: 6/21/1981, who was voluntarily deported in 2007.

13. HSI SA Carder submitted the documents to the HSI Forensic Document Laboratory (FDL) for examination. On August 17, 2018, SA Carder received the HSI FDL lab report back for the previously submitted evidence. Physical, microscopic, instrumental, and comparative examinations were conducted on the Permanent Resident card and Social Security card by a Forensic Document Examiner (FDE). The FDE found that both cards (Exhibits 1.1 and 1.2) submitted were counterfeit. The report went on to say that "This is supported by the fact that the exhibit does not conform to comparable genuine standards on file in the laboratory's reference library, does not contain genuine security features, and was not produced using correct production methods."

14. On October 9, 2018, HSI Confidential Informant #3 (CI-03) placed a consensual recorded phone call to (918) 955-1429 in the presence of HSI agents. A male subject answered the phone and CI-03 inquired about getting documents made. CI-03 asked for a social security card and a green card. The subject told CI-03 to send him a photo and the information (name, date of birth, address). No prices for the documents were discussed at that time. The phone call was then ended.

15. On October 16, 2018, CI-03 sent a text message to (918) 955-1429 in the presence of HSI agents. CI-03 texted the subject a picture and fictitious information needed for the documents. The subject then had CI-03 call him. Subject stated that it would cost $180 for a

green card (Permanent Resident Card) and social security card. Subject then wanted to meet CI-03 within the hour. HSI SA provided CI-03 $180 cash with which to make the purchase of the documents. Subject informed CI-03 to meet near 8100 South Garnett Road in Tulsa, Oklahoma. Shortly after arriving at the location, surveillance observed a subject arrive in a black 2016 Dodge Ram bearing Oklahoma tag GSZ-619. At the time of this transaction, the Ram was registered to **ALVARADO**. The subject parked next to CI-03's vehicle and CI-03 then got into **ALVARADO**'s vehicle to conduct the transaction. (See photo below: **ALVARADO** did not exit the vehicle)



16. HSI SA Carder and Task Force Officer (TFO) Tom Helm met with CI-03 after the transaction. CI-03 provided SA Carder with a green card and social security card that were purchased. CI-03 was shown a photograph of **ALVARADO** and asked if that was the subject in the truck, CI-03 stated that it was.

17. SA Carder queried the number on the social security card, 589-54-1202, using CLEAR. CLEAR showed the number belongs to a Justin Tracey DOB: 11/17/1985, who currently resides in Florida. The Permanent Resident card had USCIS number 094-981-014. SA Lelecas queried the USCIS database for that number. The number checked to an Aleksander Shabanov DOB: 12/08/1975, who was previously deported.

18. SA Carder submitted the purchased documents to the HSI FDL for examination. On October 30, 2018, SA Carder received the HSI FDL lab report back for the previously submitted evidence. Physical, microscopic, instrumental, and comparative examinations were conducted on the Permanent Resident card and Social Security card. The FDE found that both cards (Exhibits 2.1 and 2.2) were counterfeit and went on to say that "This is supported by the fact that the exhibit does not conform to comparable genuine standards on file in the laboratory's reference library, does not contain genuine security features, and was not produced using correct production methods."

19. The FDE further found that "Exhibit 1.1 from submission 1 and Exhibit 2.1 (the Permanent Resident Cards) from this submission share a common source; the features considered in this assessment include overall design (artwork), spelling and spacing errors, the same fingerprint image used in both exhibits, and the same serial number." The FDE also stated that "Exhibit 1.2 from submission 1 and Exhibit 2.2 (the social security cards) from this submission share a common source; the features considered in this assessment include overall design (artwork), planchette locations, and the same serial number."

20. In July 2019, HSI Confidential Informant #4 (CI-04), with the assistance of CI-02, sent a text message to (918) 955-1429 in the presence of HSI agents. CI-04 asked the subject

if he was still selling social security cards and green cards. The subject stated that he was and asked CI-04 to send him a photo, name and date of birth that would be displayed on the documents. CI-04 asked how much it would cost for the two documents. The subject stated it would cost $120.

21. CI-04 then received a phone call from the subject and told CI-04 that he would have the documents ready by 12:00 PM the next day. CI-04 told the subject they would be able to meet him after CI-04 got off work later in the afternoon. The subject also explained to CI-04 that a green card with an expiration date of ten years would cost an additional $50. CI-04 told the subject they just wanted the one-year card for $120.00. The subject told CI-04 to call him when CI-04 got off work the next day.

22. On July 17, 2019, the subject sent a text message to the undercover cell phone asking when CI-04 wanted to pick up the cards. SA Collins, using the undercover cellphone, responded and told the subject after 5:00 PM. Later that afternoon, CI-04 and CI-02 met with HSI agents and texted the subject at (918) 955-1429 and informed him they were ready to meet. SA Collins provided CI-04 with $120 to purchase the documents. The meeting took place near 4100 South Garnett Road at the QuikTrip. Surveillance observed an unidentified Hispanic male arrive in the **SCION**, the same vehicle from the first purchase, and pull up to the driver's side of CI-04's vehicle. The unidentified Hispanic male exited his vehicle and made a hand-to-hand exchange with CI-04 that lasted only seconds. Both CI-04 and CI-02 were in the vehicle when the exchange was made with the subject. (See below photo: Unidentified Hispanic male)

23. After conducting the transaction with CI-04 and CI-02, surveillance observed the Hispanic male walk to a vehicle parked on the other side of CI-04's vehicle and meet a Hispanic female who was seated in a maroon Camaro with Oklahoma license plate JJJ-891. SA Collins watched as the subject made a quick hand-to-hand exchange with the Hispanic female before leaving. Surveillance followed and observed the unidentified Hispanic male go to the apartment complex at 7541 South Mingo Road in Tulsa, where the **SUBJECT PREMISES** is located. (See below photo: Unidentified Hispanic male meeting with unidentified female after transaction with CI-04 and CI-02)

24. HSI SAs Collins and Lelecas met with CI-04 and CI-02 after the transaction. CI-04 gave the SAs the permanent resident card and social security card that were purchased. TFO Jeff Organ queried the number on the social security card, 445-36-6985, using CLEAR. CLEAR shows the number belongs to an Eli Robinson DOB: 3/15/1938, who died on 4/9/2003. The Permanent Resident card has USCIS number 096-866-588. SA Lelecas queried the USCIS database for that number. The number checks to a Nikita Purav Pandit from India. Her date of birth is 2/14/1985, and she is a Naturalized Citizen.

25. In late July 2019, HSI Tulsa utilized CI-01 to send a text message to (918) 955-1429 asking the subject for another green card and social security card for a relative. The subject

obliged and asked for the information. HSI Tulsa then sent a photograph and fictitious information for the cards via text message. A short time later, CI-02 made a consensual recorded call to the subject at (918) 955-1429 inquiring when the documents would be ready for pickup. The subject stated they would be ready in a couple hours and he would call when he was ready to meet.

26. Later that evening, CI-02 spoke with the subject on the phone and the meeting place was set for 4100 South Garnett Road at the QuikTrip. CI-02 was given $170 to make the purchase of the documents. The subject had stated in a previous purchase that the cost of a 10-year expiration on a green card would be $170 and one with a one-year expiration the cost would be $120.

27. After CI-02 arrived at the location, an unidentified Hispanic male arrived in the **SCION** and pulled up to the driver's side of the CI-02's vehicle. The Hispanic male exited his vehicle and a hand-to-hand exchange took place and lasted only seconds. The Hispanic male then left the area after the transaction. (See below photo: Unidentified Hispanic male delivering documents in purchase #4)

28. TFO Organ met with CI-02 after the transaction. CI-02 turned over the permanent resident card and social security card that were purchased. TFO Organ queried the number on the social security card, 461-36-6922, using CLEAR. CLEAR shows the number belongs to a Luvenia Scranton DOB: 4/19/1925, who died on 2/11/1994. The Permanent Resident card has USCIS number 094-981-908. SA Lelecas queried the USCIS database for that number. The number checks to an illegal alien, Jorge Morales Rosales DOB: 9/9/1985, who was not ordered removed.

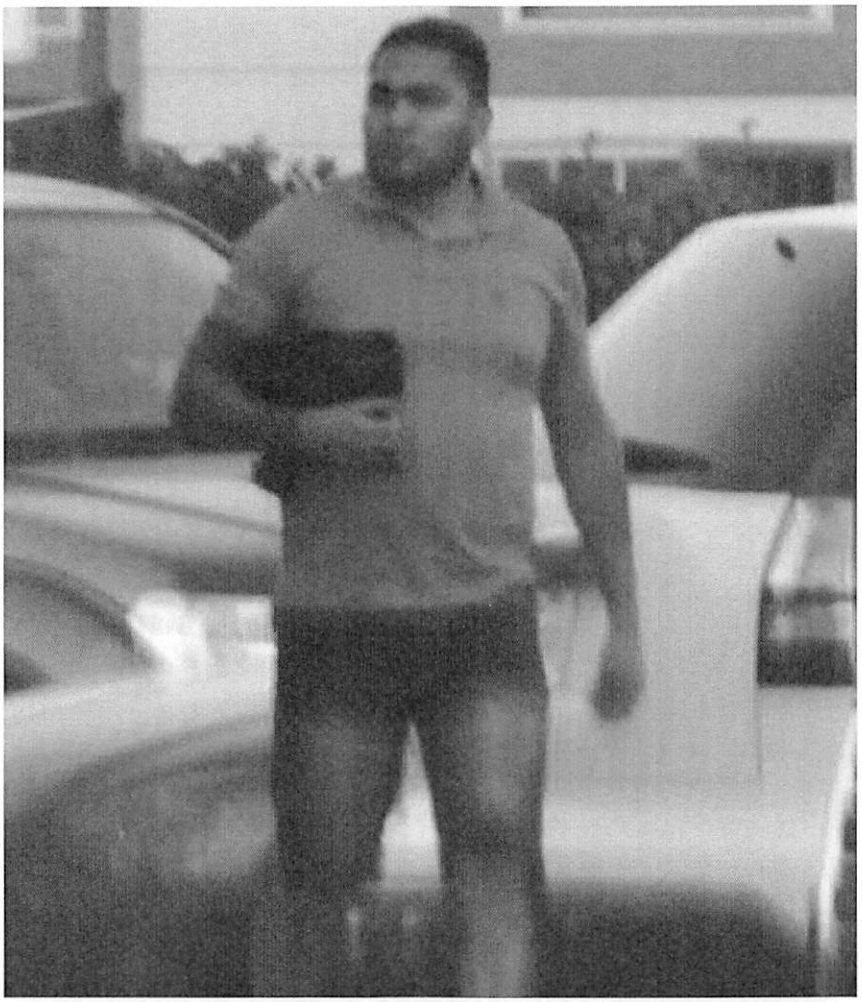
29. In mid-August 2019, CI-02 sent a consensual text message to phone number (918) 955-1429 in the presence of Special Agents Collins and Lelecas. CI-02 asked target if CI-02 could get more documents made. The target replied asking CI-02 if they wanted a $170 for a ten-year card (Permanent Resident Card) or $120 for a one-year card. CI-02 replied asking for a

ten-year card. CI-02 then texted the subject an image of a Hispanic male subject and a fictitious name and date of birth for the documents.

30. Arrangements were made for CI-02 to meet the subject at the QuikTrip near 7100 South Memorial Drive in Tulsa. CI was to call the target when CI arrived in the area. SAs Collins and Lelecas met with and briefed CI-02 at a predetermined location. CI-02 was provided with $170 USD to purchase the documents.

31. Prior to the arranged meeting, surveillance was set up at 7541 South Mingo Road at **ALVARADO**'s suspected residence. SA Carder positioned on the south side of **ALVARADO**'s apartment building, where he could see the door to the **SUBJECT PREMISES**. TFO Titsworth was positioned on the north side of the building.

32. At approximately 1950 hours, SA Carder and TFO Titsworth observed the target vehicle, the **SCION**, pull into the complex. This is the same vehicle that has been used by the suspect on multiple controlled purchases of fraudulent documents. The vehicle then parked on the north side of the building. **ALVARADO** then exited the vehicle wearing a pink-colored polo shirt, blue jean shorts carrying a blue messenger-type bag under his right arm. Surveillance observed that **ALVARADO** has a tattoo sleeve on his right arm extending all the way down to his wrist. (See below photo of **ALVARADO** walking to **SUBJECT PREMISES**)



33. Approximately one minute later, **ALVARADO** was seen walking with key in hand towards the **SUBJECT PREMISES**. **ALVARADO** then used the key to unlock the door to **SUBJECT PREMISES** and went inside, shutting the door behind him. SA Carder was able to confirm it was **ALVARADO** based on comparisons with photographs of **ALVARADO** from 2017 surveillance, his immigration A-file photograph, as well as Facebook photographs that show **ALVARADO** with a tattoo sleeve. (See below photo)

34. After being briefed by SAs, CI-02 was followed by surveillance to the meet location. CI-02 then called (918) 955-1429 and advised him that CI-02 was there. The subject advised CI-02 to park next to the air pump and that he would be there shortly. CI-02 then pulled next to the air pump and waited for the target to arrive.

35. At 2042 hours, SA Carder observed **ALVARADO** leave the **SUBJECT PREMISES** carrying the same blue messenger-type bag and walk around to the north side of the building. **ALVARADO** then got back into the **SCION** and proceeded out the west entrance/exit of the complex. SA Carder then saw the vehicle signal to turn west into the neighborhood across the street from the apartment complex. The roads in the neighborhood are often used as a shortcut to the QuikTrip and are an easy way to avoid the major traffic in the area. Surveillance was not able to catch up to **ALVARADO** in the neighborhood, but the vehicle was then seen arriving at the QuikTrip and parked next to CI-02 at approximately 2047 hours.

36. SA Collins observed the target vehicle park next to CI-02's vehicle but was not able to see the driver. A quick hand-to-hand exchange took place and then the target vehicle left the area. SA Collins then followed CI-02 back to the predetermined location. SA Carder arrived at the location as well and CI-02 was debriefed. CI-02 provided SAs Collins and Carder with the Permanent Resident Card and Social Security Card that were purchased.

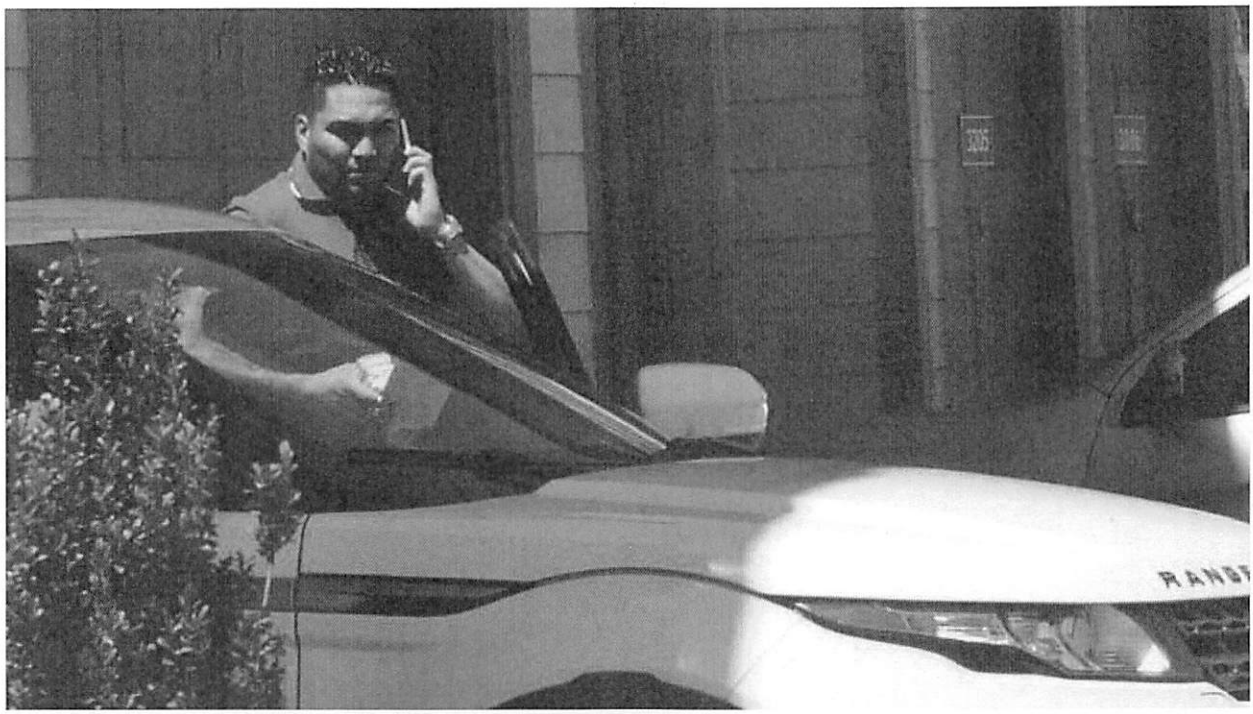
37. CI-02 stated that the subject that sold CI-02 the documents on this buy was a different individual than the subject that sold CI-02 the documents from the last buys. SA Collins inquired about what was different about the subject who sold CI-02 the documents. CI-02 stated that the subject from purchase #5 was darker skinned and heavier than the Hispanic male on the previous purchases.

38. After a comparison and review of surveillance photographs taken from all the controlled purchases of documents, photograph from **ALVARADO**'s immigration A-file, and Facebook photographs, SAs and TFOs realized that the subject that sold CI-02 the documents in purchases #3 and #4 was not **ALVARADO** as previously thought.

39. During surveillance on the August 14, 2019 document purchase, SA Carder observed **ALVARADO** enter the **SUBJECT PREMISES**. It was after a review of photographs taken during this time that agents realized **ALVARADO** has a tattoo sleeve on his right arm down to his wrist, and a tattoo on his left calf. This was the first time that these identifying features have been seen on **ALVARADO**. This can be accounted for because **ALVARADO** has not exited his vehicle when conducting the document transactions himself during this investigation. It was noted that on document purchases #3 and #4, that the unidentified Hispanic male did exit his vehicle to conduct the transactions with CI-02. The Hispanic male shared similar facial features to **ALVARADO** and surveillance believed it was him at the time. Photographs of this Hispanic male appear earlier at paragraphs 23 and 24 of this Affidavit.

40. On August 15, 2019, TFO Titsworth conducted a query of court records **ALVARADO**. TFO Titsworth located a traffic citation, TR-2019-12296, filed through Tulsa County on August 13, 2019 for **ALVARADO**. The citation showed that **ALVARADO** was operating the **LANDROVER**. A vehicle registration check showed the **LANDROVER** to be registered to Christian Morales and Angiee Moscoso Pelaez at the **SUBJECT PREMISES**.

41. Later that day, TFOs Titsworth and Warren conducted surveillance at **SUBJECT PREMISES** and observed the **LANDROVER** parked in front of an open garage door. The TFOs then observed **ALVARADO** getting into that vehicle. **ALVARADO** had his phone to his ear and was holding a stack of card-like objects in the other hand. (See photos below)



42. For every controlled purchase, phone number (918) 955-1429 has been contacted to set up the document purchases and send photos and fictitious information to in order to make the fraudulent documents. This is the number that was provided by **ALVARADO** in the beginning of the investigation.

43. Since the third and fourth controlled purchases, surveillance has consistently observed the **SCION** going back to the apartment complex at 7541 South Mingo Road after conducting the transactions. The vehicle has also been observed there during random surveillance checks. Surveillance on the fifth controlled purchased observed **ALVARADO** use

a key to enter the **SUBJECT PREMISES**. **ALVARADO** then left later driving the **SCION**, which met CI-02 to deliver the documents.

44. On August 16, 2019, SA Carder queried **ALVARADO** on the database CLEAR. CLEAR showed the **SUBJECT PREMISES** as an address associated with the subject. In addition to this and the previously mentioned LANDROVER being registered to **ALVARADO** at the **SUBJECT PREMISES**, a 2014 Chevrolet Corvette bearing Oklahoma tag GSY-092, is also registered to **ALVARADO** at the **SUBJECT PREMISES.**

45. Your affiant knows through his training, experience and working with other investigators that document vendors who manufacture, distribute, and possess fraudulent and counterfeit documents possess and/or have access to cellular phones, computers, cameras, electronic tablets and other hand-held media, thumb drives, external hard drives, other electronic storage media devices, laminating devices, printers, laminate sheets, and blank stock identification cards/sheets and these devices and equipment are often kept in their residence and/or on their person. These document vendors also typically have US currency on their person or in their residence, as this is typically a cash business.

46. Your affiant knows through his training, experience, and working with other investigators, that those who manufacture and distribute counterfeit documents often do so using cellular phones, computers, cameras, electronic tablets, and other hand-held media devices as described in this Affidavit.

47. Your affiant further knows through his training, experience, and working with other investigators, that those who manufacture and distribute counterfeit documents often use

their vehicles to store and transport counterfeit documents and other instrumentalities and fruits of their conduct.

BACKGROUND ON COMPUTERS, CELLULAR PHONES, AND THE INTERNET

48. Your affiant has had both training and experience in the investigation of computer-related crimes. Based on your affiant's training, experience, and knowledge, he knows the following:

a. Cellular phones, computers and digital technology are the primary way in which document vendors involved in the manufacture, production, distribution and possession of fraudulent and counterfeit documents communicate with potential clients. Cellular phones, computers and digital technology basically serve four functions in this regard: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. The computer's ability to store images in digital form makes the computer itself an ideal repository for the manufacture and production of fraudulent documents. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or

videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices, such as smartphones or cellular phones, can easily be concealed and carried on an individual's person.

SPECIFICS OF SEARCH AND SEIZURE OF CELLULAR PHONES, COMPUTER SYSTEMS AND OTHER DIGITAL MEDIA

49. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES** or the **VEHICLES** in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, such as a cellular phone or tablet, that are within the subject's custody, control, or accessible to the subject. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

50. Your affiant submits that if a computer, cellular phone, or storage medium is found on the **SUBJECT PREMISES** or the **VEHICLES** and is within **ALVARADO's** custody or control, or reasonably accessible by **ALVARADO**, there is probable cause to believe those records will be stored on that computer, cellular phone, or storage medium, for at least the following reasons:

a. Based on your affiant's knowledge, training, and experience, he knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via

the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

51. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** or the **VEHICLES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In your affiant's training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs,

may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. Your affiant knows that when document vendors use a computer or cellular phone to manufacture, produce, distribute, and/or possess fraudulent/counterfeit documents, the individual's computer or cellular phone will generally serve both as an instrumentality for committing the crime, and as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From your affiant's training and experience, he believes that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; and other records that indicate the nature of the offense.

52. Based upon your affiant's training and experience and information relayed to him by agents and others involved in the forensic examination of computers, he knows that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, compact disks, memory cards, memory

chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. He also knows that during the search of the premises it is not always possible to search computer equipment and storage devices for data for several reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through several methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

53. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants your affiant is applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire

medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

CONCLUSION

54. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. Your affiant respectfully requests that this Court issue search warrants for the location described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

55. Your affiant is aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab; digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Dustin L. Carder
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 22nd day of August 2019.

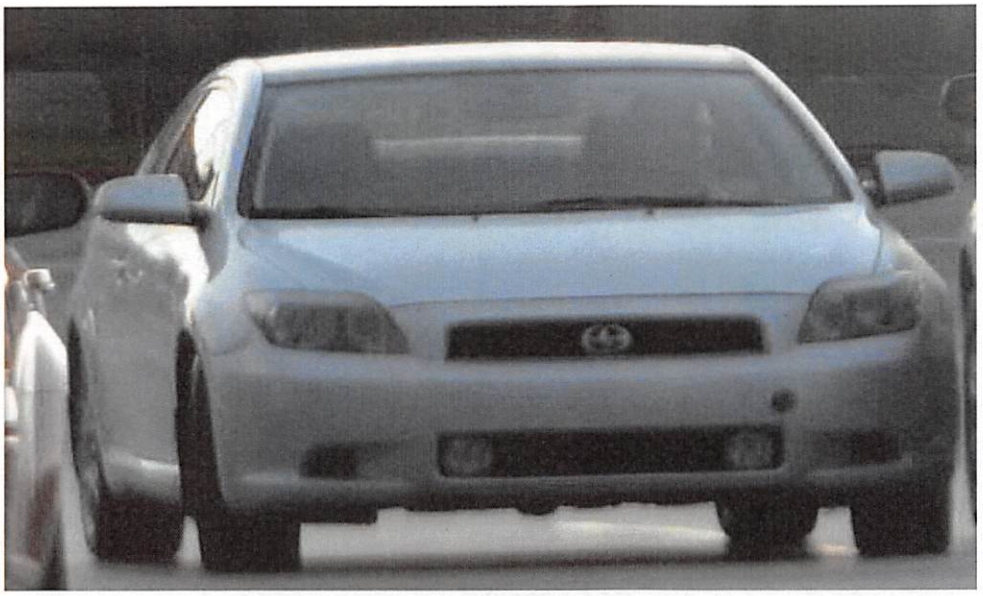
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

The entire property located at **7541 South Mingo Road, Apartment #3119, Tulsa, Oklahoma**, including the residential apartment, any garages or outbuildings assigned to apartment #3119, and any vehicles located therein (the **SUBJECT PREMISES**). The residence to be searched is located in a multi-family gated apartment complex known as the Springs at Woodlands South. The complex is located on the east side of South Mingo Road and just south of East 75th Street South. Turning into the complex from South Mingo Road, the residence to be searched is in the first building facing southwest towards South Mingo Road. The building itself is situated in a northwest to southeast position. The building is green in color with off-white siding, brown trim, and a dark-colored composite roof. The residence to be searched is in the southeast end of the building. The front door for Apartment #3119 faces the southwest and is brown in color with the numbers "3-1-1-9" in white on the door. The residence to be searched is described above and pictured below:

A 2006 Toyota Scion two-door coupe bearing Oklahoma tag CZM-657, VIN # JTKDE167060070600 (the "**SCION**"). The vehicle to be searched is pictured below:



A white 2013 Landrover 4-door Oklahoma license plate GTD626, VIN # SALVR2BG7DH855411 (the "**LANDROVER**", together with the SCION the "**VEHICLES**"). The vehicle to be searched is pictured below:

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. Books, records, receipts, notes, correspondence, ledgers, bank statements, mail and packages delivered by the U.S. Postal Service and other couriers, and other documents or papers relating to the manufacture, possession, and/or distribution of fraudulent identification documents and monetary proceeds therefrom;
2. United States currency, currency from any foreign government, and financial instruments, including certificates of deposit, stocks, bonds, and other securities;
3. Fraudulent identification documents, including but not limited to counterfeit U.S. Immigration documents, counterfeit U.S. Social Security Cards, counterfeit identification documents of foreign governments, and counterfeit state driver's licenses and ID cards;
4. Documents establishing the identity of the person or persons occupying the residence at the **SUBJECT PREMISES**, including mail correspondence, telephone, electric, and other utility statements;
5. Documents establishing ownership of the **VEHICLES**, including mail correspondence, telephone, electric, and other utility statements.
6. Address or telephone books and papers reflecting names, addresses, and telephone numbers;
7. Equipment and materials related to the manufacture, possession, and/or distribution of fraudulent identification documents, including but not limited to paper products, laminating equipment and materials, photographic equipment and materials, digital cameras, cellular telephones, computers, monitors, printers, scanners, and data storage devices, e.g., hard disk drives, thumb drives, memory chips, CD and DVD disks, zip disks, or any other electronic storage media;
8. Digital data related to the manufacture, possession, and/or distribution of fraudulent identification documents stored on a variety of systems and storage devices, including digital cameras, cellular telephones, computers, monitors, printers, scanners, and data storage devices, e.g., hard disk drives, thumb drives, memory chips, CD and DVD disks, zip disks, or any other electronic storage media, and related software, documentation, and data security devices (including passwords) that are reasonably believed to be within the

possession, custody, control, or access of Christian Alvarado Morales, so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment;

9. To enable a qualified computer expert to accurately retrieve digital data in a laboratory or other controlled environment, Affiant requests the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude it would be impractical to search the computer hardware on-site for this evidence.